Computer Security

Firewalls

What is a Firewall?

fire wall
1 : a wall constructed to prevent the spread of fire
2 *usually* **firewall :** a computer or computer software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users (as of the Internet)

What is a Firewall?

- A *firewall* is a kind of *filter* or *barrier* that affects the message traffic passed between two networks
- Often used as a perimeter defense
  - Allows an organization to choose which protocols it will exchange with the outside world.
- Can also be used to block access to certain Internet sites
  - To prevent employees from downloading from blacklisted servers
  - To prevent employees from accessing porn sites, etc.
- Usually, blocks outsiders from accessing the internal network.
- Sometimes, protects against internal users connecting with the Internet.

What is a Firewall?

- It is important to realize that a network firewall shares something in common with its physical cousin:
  - A physical fire wall is designed to *slow down* the spread of a fire. It does *not prevent* the spread of a fire.
- A network firewall should be be viewed in the same way:
  - It is not a complete solution
  - Other measures must also be employed.

What Firewalls Can Do*

- Can be a single "choke point" to:
  - keep unauthorized users out of the protected network
  - prohibit potentially vulnerable services from entering or leaving the network
  - provides protection from various kinds of IP spoofing and routing attacks
  - simplify security management by consolidating onto a single system
- Provides a location for monitoring security-related events
  - Audits and alarms can be implemented on the firewall
- Provides a convenient platform for several security-related Internet functions, including:
  - Network address translator, to map local addresses to Internet addresses
  - Network management to provide audits or logs of Internet usage
- Can serve as the platform for IPSec.
  - Can be used to implement virtual private networks (VPNs)

*_Cryptography and Network Security_, by William Stallings, published by Prentice-Hall.

What Firewalls *Cannot* Do*

- Protect against attacks that bypass the firewall.
  - Dial-out / dial-in systems for employees and telecommuters
- Protect against internal threats
  - A disgruntled employee
  - An unwitting employee cooperating with attacker
- Protect against the transfer of virus-infected programs or files.

*_Cryptography and Network Security_, by William Stallings, published by Prentice-Hall.

Types of Firewalls

- Hardware-based
  - Integrated "appliances" that include all of the hardware and software necessary to implement the firewall
  - Typically have much better performance than software-based firewalls
  - Vendors include Cisco, et. al.
- Separate host
  - Operating System / Software combination
  - Often a Unix box with perhaps additional software
- Local software
  - Typically a personal firewall
  - Vendors: Symantec, Zone Labs, etc.

Types of Firewall

- ***Packet-Filtering Firewall***
  - a.k.a. ***Screening Firewall***
- ***Stateful Inspection Firewall***
  - a.k.a. ***Stateful Packet Filter Firewall***
- ***Application-Level Gateway***
  - a.k.a. ***Application Proxy*** or ***Application-level Proxy***
- ***Circuit-Level Gateway***

Packet Filtering Firewall

- Basically a router with a set of filters to determine which packets will are allowed to cross the boundary
  - Operates at the Network Layer (Layer 3) and Transport Layer (Layer 4)
  - Looks at the IP and TCP packet headers, and applies a set of configurable rules to either discard or forward the packet.

Packet Filtering Firewall

- The rule configurations include:
  - Source IP address
  - Destination IP address
  - Source and destination transport-level address
  - IP protocol fields
  - Router interface port (source or destination)

Packet Filtering Firewall

- Can be subject to the following attacks:
  - IP address spoofing
    - Falsifying the source IP address
  - Source Routing attacks
    - Attempts to bypass security measures that do not analyze the source routing information
  - Tiny fragment attacks
    - Uses the IP fragmentation option to create extremely small fragments and force TCP header information into a separate packet fragment.
    - Attempts to circumvent filtering based on TCP header information.

Stateful Inspection Firewalls

- Packet filtering firewalls analyze individual packets, and are not capable of maintaining connection state information.
- ***Stateful Inspection Firewalls*** maintain data about open connections to ensure that packets are part of a valid connection initiated by an authorized user.
  - Tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, one entry per connection.
  - Once a connection is in the directory, the packet filter will allow incoming traffic to high-numbered ports only for those packages that fit the profile of one of the connections in the directory.

Application-Level Gateway

- An ***Application-Level Gateway***, also called a ***Proxy Server***
  - Acts as a relay of application traffic
  - Conversation looks like:
    - The client contacts the gateway using a certain TCP/IP application protocol such as Telnet, FTP, etc.
    - The gateway asks the client for the name of the remote host to be contacted.
    - The user responds, and provides a valid user IT and authentication
    - The gateway then contacts the application on the remote host, and relays TCP segments containing the application data between the two end points
  - If the gateway does not implement the code for a specific protocol, then that protocol is not supported
  - The gateway can also be configured to support only specified features of a protocol that are considered acceptable.

Application-Level Gateway

- Pros:
  - Tend to be more secure than packet filters
  - User authentication allows for effective blocking of unwanted traffic
  - Easy to log and audit all incoming traffic at the protocol level.
- Cons:
  - Requires additional processing overhead for each connection
  - Effectively two connections between end users
  - Still susceptible to SYN floods and ping floods

Circuit-Level Gateway

- A ***Circuit-Level Gateway***
  - Can be:
    - a stand-alone system, or
    - a specialized function performed by an Application-Level Gateway for certain applications
  - Does not permit an end-to-end TCP connection; instead, it sets up two TCP connections:
    - Between itself and a TCP user on an inner host
    - Between itself and a TCP user on an outside host
  - Before the connections are set up, the user must be authenticated
  - Once the connections have been established, TCP segments are conveyed between the two without examining the segment contents
  - The security consists of determining which connections are allowed.
  - Can be configured to support application-level services on inbound connections, and circuit-level functions for outbound connections

Circuit-Level Gateway

- Pros:
  - Relatively secure
- Cons:
  - May not be appropriate for some public situations
  - Typically does not support certain features, such as URL filtering
  - Often only offer limited auditing features.

Firewall Topologies

- ***Bastion Host***
- ***Screened Subnet***
  - a.k.a. ***Demilitarized Zone (DMZ)***
- ***Dual Firewalls***

Bastion Host

- Places the firewall at the perimeter of the network
  - The sole link between the protected network and the outside world
  - All traffic flowing in and out of the network must pass through the firewall
  - Easiest topology to implement, and the least expensive

bas·tion
1 : a projecting part of a fortification
2 : a fortified area or position
3 : something that is considered a stronghold

Screened Subnet (DMZ)

- Still uses a single firewall, but with three network interface cards:
  - One connected to the external network
  - One connected to the protected network
  - One connected to a ***Screened Subnet***
- A ***Screened Subnet:***
  - Provides a middle ground that serves as neutral territory between the external and protected networks (hence the term DMZ)
  - Will contain servers that provide services to external users:
    - Web servers, SMTP servers, etc.
  - Allows servers to be compromised without compromising the protected network.

Dual Firewalls

- Also provides a DMZ that may be used to house public services
  - Replaces a single firewall having three NICs with two firewalls each with two NICs
- Provides similar security benefits as the Screened Subnet approach, plus minimizes the likelihood that an attacker could compromise the firewall itself.
- To enhance this, can use two very different firewalls:
  - A hardware firewall + a software firewall
  - Firewalls from two different vendors
  - Firewalls with different levels of security certification

Other Firewall Features

- Two features that are commonly supported by firewalls are:
  - ***Network Address Translation (NAT)***
  - ***Virtual Public Networks (VPNs)***

Network Address Translation (NAT)

- ***NAT*** is a kludge that has allowed the Internet to survive with only 32-bit addresses
- NAT allows you to allocate IP addresses to your own private network, and prevent the outside world from every seeing them
- In RFC 1918, IETF set aside some address ranges for creating private networks:
  - **`10.x.y.z`**
  - **`172.16.y.z`**
  - **`192.168.y.z`**

  These IP addresses are "unroutable", and will be dropped by any router on the Internet.

Network Address Translation (NAT)

- When you wish to communicate between a private network host, and the Internet, the internal IP address is translated to an IP address that is acceptable to the Internet, using a ***Network Address Translation (NAT)*** device
- Possibilities include:
  - Mapping to a single external IP address
    - All traffic appears to be coming from the NAT device's IP address
    - Commonly used to connect a large network to the Internet when a limited number of IP addresses is available
  - 1-to-1 mapping
    - Each machine in the internal network could have its own unique external IP address
  - Dynamically allocated address
    - The NAT device could multiplex a large number of unroutable IP addresses to a smaller number of valid external IP addresses

NAT Security Benefits

- Firewalls often implement NAT
- Helps to hide the internal network's internal IP address usage
- By itself, NAT offers few security benefits, so NAT must be combined with a secure firewall implementation to maintain adequate security

Virtual Public Networks (VPN)

- Many firewalls support ***Virtual Public Networks (VPNs)***
- A VPN allows a user access from outside a firewall via a *"tunnel"*, and as a result appear to actually be inside the internal network.
  - A tunnel is a point-to-point connection where the actual communication occurs across a network.
- Used to allow users who work from home or on the road to access their work systems in a secure fashion.
- VPN typically uses IPSec to encrypt the communications, using a modern block cipher, and thereby make eavesdropping extremely difficult

Summary

- We've discussed:
  - The principles of firewalls, what they can do, and cannot do
  - The different kinds of firewalls
  - The various firewall topologies
  - Additional functionality often supported by firewalls
- This was not a complete, comprehensive treatment of firewalls. To learn lots more detail about firewalls, see:

  Building Internet Firewalls (2nd Edition)
  by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
  Publisher: O'Reilly (January 15, 2000)
  ISBN: 1565928717